Campaign 2008

Innovative Ideas for Securing America

A GUIDE FOR CANDIDATES

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 SEP 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Campaign 2008: Innovative Ideas for Securing America, A Guide for Candidates	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Business for National Security,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**34**	

Campaign 2008

Innovative Ideas for Securing America

A GUIDE FOR CANDIDATES

Business Executives for National Security • www.bens.org

Dear Candidate:

This election, voters are demanding creative, new approaches to the urgent national security challenges facing the United States.

With the record-high cost of oil and gas, how can our nation—and our military—reduce its dependence on imported foreign oil?

With American servicemen and women serving in Iraq and Afghanistan, how can we equip our troops with the most advanced tools and technologies so they can survive and succeed on the battlefield?

With our country engaged in a global fight against terrorism, how can we prevent future attacks by strengthening U.S. intelligence operations, tracking terrorist financing and preventing weapons of mass destruction from falling into the hands of terrorists?

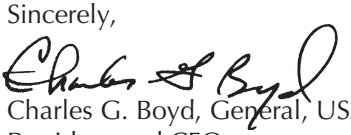
With terrorists still seeking to strike U.S. soil, how can we protect and defend the American homeland—our ports, our critical computer networks and our local communities?

As voters look to you for answers to these and other critical questions, Business Executives for National Security (BENS)—a national, nonpartisan group of business leaders—invites you to consider the innovative approaches offered in this guidebook.

For more than 25 years, BENS has worked with administrations from both political parties to help build a more secure America by tapping the insights, expertise and best practices of the private sector. Our information and policy recommendations have been embraced by Democrats and Republicans alike.

If you need additional information on any of the topics in this guide, please visit our website at www.bens.org or contact us at (202) 296-2125, fax (202) 296-2490, or email at bens@bens.org.

Sincerely,



Charles G. Boyd, General, USAF (Ret.)
President and CEO
Business Executives for National Security

Table of Contents

National Security is Everybody's Business 4

Building Partnerships to Strengthen Homeland Security 6

Preventing the Spread of Weapons of Mass Destruction 8

Defending Against Cyber Attacks 10

Combating Terrorist Financing 12

Increasing America's Energy Security 14

Securing America's Ports 16

Transforming the Intelligence Community 18

Improving Homeland Security Oversight 20

Buying Smarter at the Pentagon 22

Revitalizing Military Bases 24

Recruiting and Retaining the Best People for Government Service 26

Harnessing the Full Strength of America to Promote Global Security 28

Business Executives for National Security 30

Board of Directors 31

Contact Information 32

National Security is Everybody's Business

"But what can I do?"

That's the question many Americans ask themselves when it comes to keeping the United States strong and safe. After all, isn't dealing with national security threats the responsibility of government? Isn't fighting and winning wars the military's job? Isn't responding to domestic emergencies a task for states and emergency officials?

In fact, with today's threats and challenges—to our national security, our homeland security, our energy security—keeping America strong and safe is no longer the sole responsibility of the government and military. Every citizen has an opportunity—and a responsibility—to help.

The private sector has a unique opportunity to contribute. The same entrepreneurial spirit that has transformed American business in recent decades can help transform the business of national security—how the United States government and our armed forces meet and defeat the security threats to our country.

"We must spend as much as necessary to protect the American people, but do so carefully and wisely, and constantly endeavor to find new and better ways of doing business—first and foremost, for the man or woman fighting on the front lines, but also for the taxpayer at home."
— Secretary of Defense Robert M. Gates,
BENS Eisenhower Award Dinner, May 15, 2008

Keeping America Strong

To meet the security challenges of our time, our government—including our military—must be structured and strengthened to ensure that it is capable of responding quickly and decisively to the missions of the 21st Century. The same entrepreneurial spirit that has strengthened American businesses in the global economy can help strengthen our national security apparatus. For example:

- The same business practices that have allowed American business to improve efficiency and reduce costs can help the Pentagon ensure that U.S. forces get the equipment they need faster, better and cheaper and reduce its dependence on foreign oil.

- The same management principles that have enabled American executives to streamline and strengthen their companies can help the U.S. Intelligence Community reduce bureaucratic barriers and increase cooperation among intelligence agencies.
- The same business and civilian expertise that has driven economic growth and created jobs in the U.S. can be harnessed to rebuild and revitalize strife-torn societies abroad.

Keeping America Safe

Protecting our nation against terrorist attacks or natural disasters is too massive a task for government alone. With most of America's critical infrastructure – ports, telecommunications, energy and water supplies – controlled by the private sector, business must be a partner in preventing, preparing for and responding to catastrophic events. For example:

- With their vast array of facilities, vehicles and employees, private companies can help federal, state and local governments respond to domestic emergencies.
- With virtually all U.S. overseas trade passing through the nation's two dozen major ports, industry can help devise security procedures that keep ports open for business but closed to terrorists.
- With the U.S. economy and armed forces critically dependent on information systems that are vulnerable to attack, the private sector can help devise cyber security policies that are both effective and economically viable.

"Government agencies are responsible for protecting the lives and property of their citizens and promoting their well-being. However, government does not, and cannot, work alone. Private sector organizations play a key role before, during and after an incident."
— The National Response Framework,
Department of Homeland Security, January 2008

The following pages offer innovative solutions to these and other urgent national security challenges facing the United States, drawing on the experience and proven practices of the private sector. Because – now more than ever – national security is everybody's business.

Building Partnerships to Strengthen Homeland Security

The Challenge:

- Securing the homeland is a responsibility shared by many: every level of government, civic leaders, the military, non-governmental organizations, the business sector, and individual citizens.
- The initial impact of any catastrophe is local, and that is where we must build robust new security capabilities and greater community resilience – providing a strong first line of defense during a crisis.
- Key to comprehensive, effective disaster management and recovery is organization, communication, and regular exercises involving all the players on the response team: a true partnership.

"We had to fight for fuel with the government and [other companies] – even though we were all on the same team. We're all calling to the same five guys to get the same things. It would be far better if there were a pre-positioned supply chain."

— Robert S. Boh, Pres. & CEO, Boh Bros. Construction Co., LLC, 2006, after Hurricane Katrina

The Current Approach:

- While there is broad support for the concept of public-private collaboration, the resources and expertise required to implement and sustain these partnerships too often fall short.
- West Coast wildfires, East Coast hurricanes, and Midwest floods have demonstrated the importance of building "ground-up" partnerships, but given many different models and programs, partnerships cannot always communicate and coordinate their efforts on a larger scale.
- Federal regulations inhibit speedy response to disaster stricken states, and temporarily lifting these regulations is frequently time consuming.
- Because "Good Samaritan" laws vary from state to state and generally apply only to individuals, not corporations, companies are often reluctant to help in disaster response for fear of lawsuits.

A New Approach:

- Make private sector support to disaster response a reality by including business in disaster planning and by encouraging—and funding when necessary—private sector participation in training and exercises.
- Create an independent, non-partisan public benefit corporation dedicated to building resilience by facilitating public-private collaboration, and enabling a nation-wide network of community, state, and regional partnerships.
- Establish procedures in the executive branch that quickly roll back federal regulations that obstruct private sector assistance in disasters.
- Work at the state level to extend application of Good Samaritan laws to organizations and corporate entities.

"The Federal government should recognize that the private/non-government sectors often perform certain functions more efficiently and effectively than government because of the expertise and experience in applying successful business models. These public-private partnerships should be facilitated, recognized, funded [and]. . . the capability to draw on these resources should inform and be part of Federal, State, and local logistics systems and response plans."

— The Federal Response to Hurricane Katrina: Lessons Learned, The White House, February 26, 2006

Frequently Asked Questions:

Why hasn't business been integrated more fully in local, state, and federal disaster management and homeland security operations?
Businesses are eager to help their communities and the nation during crisis, but there are legal, regulatory, and jurisdictional barriers that can limit their ability to do so. Federal policy should promote self-managed community or statewide partnerships, while minimizing inter-governmental and policy conflicts that discourage effective collaboration.

What is the advantage of the proposed public benefit corporation?
Government programs cannot mandate public-private collaboration. An independent, non-governmental entity can serve as a national resource for helping businesses, government, non-profit organizations, and communities establish and sustain public-private partnerships that strengthen American security.

Preventing the Spread of Weapons of Mass Destruction

The Challenge:

- In Russia and other countries around the world, poorly guarded nuclear, biological and chemical weapons and materials make tempting targets for terrorist groups like al Qaeda, which has threatened to obtain and use them against the United States and its allies.
- An attack on a major U.S. city with a weapon of mass destruction could kill or injure hundreds of thousands of Americans and inflict hundreds of billions of dollars in damage.
- Major arms control treaties – which include limits on and provisions for monitoring weapons of mass destruction – are expiring without replacement, leaving these weapons, and the United States, vulnerable.

"Today, al Qaeda's nuclear intent remains clear. Osama bin Laden said in 1998 that it was an Islamic duty to acquire weapons of mass destruction. Past experience strongly suggests that they are seeking an attack more spectacular than 9/11."
— Rolf Mowatt-Larssen, Director of the Energy Department's Office of Intelligence and Counterintelligence, April 2008

The Current Approach:

- Despite the major threat that poorly guarded nuclear, biological and chemical arsenals pose to the United States, annual administration budget requests for key U.S. nonproliferation initiatives have stagnated over the last four years.
- U.S. government assistance has kept former Soviet weapons scientists employed – and their expertise "off the market" – for the short term, but doesn't transition these individuals to peaceful pursuits outside state-run weapons labs.
- With no real effort underway to renew the START treaty – a cornerstone of nuclear arms control with Russia – the treaty will expire in 2009, and the U.S. will lose its underlying authority for monitoring Russian arsenals and securing and destroying vulnerable Russian weapons.

A New Approach:

- The next administration and Congress should work together to increase funding for vital Defense and Energy Department programs that have already secured enough vulnerable uranium worldwide for two dozen nuclear bombs and destroyed thousands of poorly guarded weapons of mass destruction in Russia and the former Soviet states.
- In partnership with the business community, the U.S. government should explore new approaches to creating long-term, self-sustaining private-sector opportunities for former Soviet weapons scientists, outside of state weapons institutes.
- The next administration and Congress should move urgently to renew the START treaty as the foundation for limiting and monitoring nuclear arms and continuing nonproliferation efforts to keep weapons of mass destruction out of terrorist's hands.

Under the Nunn-Lugar Cooperative Threat Reduction program, 7,266 former Soviet nuclear warheads have been deactivated, 1,312 ballistic missiles have been destroyed, and over a thousand missile silos, strategic bombers, cruise missiles, and submarine missile launchers have been decommissioned.
— Defense Threat Reduction Agency Nunn-Lugar Scorecard, 2008

Frequently Asked Questions:

How likely is it that a terrorist could develop or steal a weapon of mass destruction?
While developing, buying, or stealing a weapon of mass destruction remains difficult and costly, terrorist groups like al Qaeda have demonstrated that they have the will and funds to try. Without U.S. programs to help secure them, nuclear and radiological materials in countries around the world and old Soviet stockpiles of deadly weapons will remain dangerously at-risk.

Shouldn't other countries secure and destroy their own weapons arsenals?
Destroying thousands of Cold War-era weapons, and securing weapons-grade nuclear material scattered around the globe, is too costly and complicated for any one country alone. Spending a small fraction of our foreign affairs and defense budgets to secure these weapons is a cost-effective investment in our own security: every nuclear, biological, or chemical weapon eliminated overseas is one less weapon that could be used to attack the U.S.

Defending Against Cyber Attacks

The Challenge:

- America's dependence on computers and networked information systems leaves every aspect of our society – including government, the military and business – increasingly vulnerable to a cyber attack.
- Hackers – many of them overseas – are increasingly probing, penetrating and trying to disrupt U.S. government and private sector computer systems. More worrisome is the prospect that terrorists or hostile nations could trigger a large-scale shutdown of national computer networks – an "electronic Pearl Harbor."
- The private sector, which owns and operates most of the information networks in the U.S., must be a partner with government in addressing this threat.

"The reality is that the Defense Department is constantly under [cyber] attack ... It will come as no surprise that we aggressively monitor intrusions and have appropriate procedures to address events of this kind. We get perhaps hundreds of attacks a day."
— Secretary of Defense Robert M. Gates, June 2007

The Current Approach:

- The government has often attempted to dictate terms and cyber security regulations to the private sector, rather than forging a true partnership with industry that welcomes the full insights of the private sector.
- Despite some progress in recent years, overall responsibility for national cyber security policy and structures is still spread too widely through the executive branch – with too little coordination between agencies and with the private sector – and congressional oversight of cyber security policies remains spread across multiple committees.

A New Approach:

- Government and business should work together to:
  - Build awareness among corporate leaders that cyber attacks are increasing, particularly foreign-sponsored commercial cyber-espionage;
  - Establish means to better identify vulnerabilities and actual cyber threats; and
  - Develop plans and procedures to help recover from attacks.
- Rather than dictating rules and regulations, government should take a more collaborative approach to cyber security and engage the computer security industry's expertise. Better information sharing will aid law enforcement efforts and help to identify best preventive practices.

"The Federal government [should] strengthen its cyber security technology transfer partnership with the private sector, jointly sponsor with the private sector an annual interagency conference at which new cyber security R&D results are showcased, [and] fund technology transfer efforts in cooperation with industry by researchers who have developed promising ideas or technologies."
— President's Information Technology Advisory Council
"Cyber security: A Crisis of Prioritization" February 2005

Frequently Asked Questions:

Wouldn't it be easier if the U.S. government and private sector each simply focused on protecting their own computer networks?
Neither government nor business can address this challenge alone. Most of the nation's computer networks are owned and operated by private industry. But only government – which enforces relevant laws and regulations – has the intelligence resources vital to disrupting foreign-sponsored or terrorist-originated cyber attacks. Addressing cyber threats requires close and continued cooperation between both parties.

Which agency of government is ultimately responsible for cyber security?
Currently, none; different federal agencies have different (and sometimes overlapping) policy and operational responsibility for maintaining the security of federal governmental cyber assets and protecting the security of non-governmental cyber networks. While it's neither desirable nor feasible for any single agency to have sole responsibility, greater coordination across government – and with the private sector – is essential.

Combating Terrorist Financing

The Challenge:

- As they did in the 9/11 attacks, terrorist organizations use America's open financial system to raise and disseminate funds—using legitimate commercial and charitable means and illicit means like money laundering.
- Tracking and stifling the flow of money to and from terrorist groups is a proven method for undermining their ability to recruit, train, and conduct operations.
- Uncovering and tracking terrorist funds requires the cooperation of the financial services industry, including banks, insurance firms and money-service businesses.

"Many of the threats we face – from terrorism to the proliferation of weapons of mass destruction to narcotics trafficking – all have one thing in common: they rely on financial support networks. These threats are ...asymmetric and borderless and thus not necessarily susceptible to being solved exclusively by traditional means of deterrence."

— Under Secretary for Terrorism and Financial Intelligence Stuart Levey, Testimony before The Senate Committee On Finance, April 1, 2008

The Current Approach:

- Despite some reforms, the time-consuming procedures by which the private sector is required to alert the federal government of suspicious financial activities are often incapable of generating the quick action needed to catch, track, or block terrorist-supported financial transfers.
- Even after significant investments, the federal government's outdated information technology systems cannot effectively process and utilize data collected from the financial services industry.
- With over a dozen agencies involved, the U.S. government lacks a central authority to effectively coordinate tracking of terror financiers and cooperation with the private sector.

A New Approach:

- To identify suspicious financial activities faster, government and the financial-services industry should continue working to improve and strengthen communication and information sharing.
- To move quickly when suspicious activities are identified, the federal government, with help from the financial community, should modernize its information technologies and update regulations in keeping with private-sector advances.
- To improve coordination among government agencies on programs that target terrorist funding, a central authority should be designated to manage U.S. terrorism finance tracking efforts.

"Our financial actions have produced demonstrable impacts on threats ranging from terrorist groups to narcotics cartels, and on dangerous regimes in North Korea and Iran. This new strategy uses conduct-based, intelligence-grounded, targeted financial measures to harness the power of the private sector...adding an innovative financial dimension to our national security effort."
— Treasury Secretary Henry Paulson, June 2007

Frequently Asked Questions:

How successful has the United States been in tracking and blocking terrorist funds?
The federal government has made disrupting terrorist financial networks a high priority since 9/11, and by following the money, has saved lives by tracking and arresting terrorism suspects and thwarting acts of terrorism. Many of those success stories are the result of inter-agency and international cooperation. However, the lack of greater federal coordination – and rapid information-sharing with the private sector – leaves much room for improvement.

But won't greater government access to financial records undermine privacy?
Not necessarily. Even though federal laws and regulations require financial institutions to report suspicious financial activities, the Right to Financial Privacy Act sets procedures for federal access to customer financial records and generally requires that customers be notified when federal authorities seek access to their financial information.

Increasing America's Energy Security

The Challenge:

- As today's record-high gas prices remind us, the United States remains highly dependent upon oil, which accounts for more than 40 percent of America's energy consumption.
- Nearly two-thirds of the oil consumed in the U.S. is imported, much of it from countries hostile to U.S. interests or vulnerable to political or economic instability.
- Due to increasing global demand and depleted supplies, the high price of oil will continue to increase, restricting U.S. economic growth and directly impacting military readiness.

Every $10 per barrel rise in the price of fuel costs the Defense Department an extra $1.3 billion per year.
— Defense Department Energy Security Task Force, January 2007

The Current Approach:

- America's oil dependence requires a sizeable and costly U.S. military presence to stabilize oil-producing regions of the world and to secure key waterways, such as the Persian Gulf, that are highly vulnerable to a terrorist attack.
- Such an attack could disrupt supply and possibly trigger an energy crisis.
- Reducing America's dependence on foreign oil has not been a top U.S. foreign and national security priority.
- The Department of Defense, which is world's single-largest consumer of oil, lacks a strategic or unified plan to manage energy consumption across the armed forces.

A New Approach:

- The federal government should increase investments in new energy technologies, expand the use of alternative fuels, establish higher efficiency standards in vehicles, buildings, and household appliances, and expand environmentally-responsible domestic exploration and nuclear energy production.
- The next administration should give the Secretary of Energy a seat at National Security Council meetings and ensure the Secretary is consulted in relevant foreign and national security policy decision-making.
- The U.S. should work with other nations to improve security for existing refineries, pipelines, and transportation routes and offer counter-terrorism expertise and training to at-risk oil-producing nations to enhance security.
- The Pentagon should become a national model for energy efficiency by investing in and embracing energy efficient technologies and practices.

"Current events only serve to confirm the unacceptable security risks created by our extraordinary level of oil dependence. Significantly reducing the projected growth in U.S. oil consumption must become a compelling national priority."
— General P.X. Kelley, 28th Commandant, U.S. Marine Corps (Ret.), August 2006

Frequently Asked Questions:

Is total energy independence possible?
Almost certainly not, at least for several decades. Our short-term focus, therefore, must be on developing strategies to better manage the consequences of our continued dependence on oil – particularly oil from unstable foreign regions. At the same time, America must begin the long-term process of transitioning to an economy that is less reliant upon petroleum.

Is the Department of Defense doing a good job of managing its energy usage?
While the Pentagon is working to manage its relatively small energy usage at bases, less is being done to reduce consumption by combat forces – which accounts for the vast majority of defense energy needs. Also, a recent study found that no senior-level officials are directing a comprehensive Pentagon energy plan.

Securing America's Ports

The Challenge:

- With more than a quarter of U.S. gross domestic product dependent on overseas trade, the U.S. economy is critically dependent on the free flow of goods through our nation's ports.
- An estimated 11 million shipping containers pass through America's ports every year, a number that may double by 2025 – yet very little of this incoming cargo undergoes physical inspections.
- A terrorist attack on just one of America's two dozen major ports – many located in or near major urban areas – could cause enormous civilian casualties and do billions of dollars of damage to the U.S. and global economies.

"In 2002, longshore workers across the West Coast were locked out for 10 days over a contract dispute. The shutdown cost the nation's economy an estimated $1 billion to $2 billion a day."
— Associated Press, July 2007

The Current Approach:

- While the Department of Homeland Security and U.S. Coast Guard have taken steps to identify suspicious cargo before it reaches our shores, American ports remain vulnerable to weapons of mass destruction hidden aboard ships – particularly smaller vessels that are far less likely to receive scrutiny.
- Although U.S. Customs and Border Patrol officers are stationed at 58 ports overseas, the standards and technologies used at those ports for identifying high-risk cargo can vary widely.
- The Coast Guard has plans to deter and respond to terrorist attacks at ports, but these do not sufficiently focus on recovery issues, including a process for reopening a port after an attack.

A New Approach:

- To improve screening of U.S.-bound cargo at foreign ports, the U.S. and foreign governments should collaborate more closely with the business community, including multinational branches of global shipping firms, and share security best-practices and technologies.
- To focus screening efforts on high-risk containers, government and industry should work together to improve the collection, sharing, and analysis of critical information and intelligence.
- To help ports and affected communities quickly recover from terrorist attack, the federal government and industry should work together to develop clear safety standards and lines of authority for reopening ports after an attack.

"Government officials are unable to protect things ... over which they have limited jurisdiction, and the market, left on its own, is unlikely to provide the socially desired level of security and dependability. What is required is a truly collaborative approach which engages civil society and taps extensive private-sector capabilities and ingenuity for managing risk and coping with disasters."
— Stephen E. Flynn, Council on Foreign Relations, May 2008

Frequently Asked Questions:

What would be the impact of a terrorist attack on our ports?
An attack on one American port would almost certainly lead to an immediate shutdown of all our ports for an undetermined duration. Instantly, the flow of trade into and out of the U.S. would be halted, crippling our heavily trade-dependent economy and impacting every American in the form of food and product shortages and higher prices.

Can't we just inspect every container that arrives at our ports?
With 11 million shipping containers arriving at our ports each year, it is neither feasible – nor desirable – to open and examine every one. But by working together and utilizing the latest technological innovations to identify the high-risk containers most likely to pose a threat, government and industry can protect our ports without bringing our national economy to a halt.

Transforming the Intelligence Community

The Challenge:

- To successfully protect our nation's security, our leaders and armed forces need accurate and timely intelligence about America's adversaries.
- Despite reforms in recent years, unnecessary bureaucratic barriers – and the challenge of recruiting and retaining intelligence professionals – continue to limit the effectiveness of the 16-agency U.S. Intelligence Community.
- While Congress – the Intelligence Community's "board of directors" – does spend significant time on intelligence issues, that focus is often on short-term challenges and not long-term management.

"The need to produce analytical reports, analytical assessments that address real issues, provide insight, enhance understanding and improve decision-making, I think, is readily apparent, and nobody should argue contrary to that. All of this is aimed at providing better support...It's to make the performance of our government officials and agencies better. The task to do this involves better integrating the community."

— Thomas Fingar, Chairman of the National Intelligence Council, March 2008

The Current Approach:

- Despite the creation of the position of Director of National Intelligence to coordinate U.S. intelligence efforts, this official still lacks the full range of budgetary and management authority required to lead the Intelligence Community.
- Bureaucratic barriers – including a cumbersome security clearance process, outdated personnel and compensation systems, and difficulties in rotating employees across agencies – hamper the Intelligence Community's ability to recruit and retain the next generation of intelligence professionals.
- Congress offers its leadership to the Intelligence Community on "cloak and dagger" intelligence operations issues but is less involved in addressing key challenges in the day-to-day operations of the agencies it oversees.

A New Approach:

- As in any effective business enterprise, the Director of National Intelligence – our nation's intelligence CEO – must have control of the organization's management and budget, and the subsidiaries must be able to share information across institutional boundaries.
- The Intelligence Community has made some initial progress on improving security clearance, human capital, and compensation processes, but it must sustain those efforts and do more to reform each of these areas.
- Congressional oversight should take a more business-like approach to oversight of intelligence, focusing more closely on less-glamorous – but no less critical – operational issues such as management, finance, budgeting, personnel, and acquisition reform.

"It will be difficult to accomplish any of our objectives with antiquated business practices and systems. We need to deploy an integrated planning, programming, budgeting, and performance management process that aligns strategy to budget, budget to capabilities, and capabilities to performance."
— Director of National Intelligence J. Michael McConnell, February 2008

Frequently Asked Questions:

If we're at war, why should we be talking about mundane topics like human capital reform and budgeting?
The long-term health of the Intelligence Community depends on the "back office" operations that allow people in our intelligence agencies to do their jobs. "Cloak and dagger" issues typically garner public and media attention, but without reforms to their day-to-day operations, the agencies will face increasing challenges to the successful performance of their missions.

Are business models for recruiting and retaining professionals appropriate for the unique requirements of the intelligence world?
Yes. Many of the lessons of successful business can be applied to the management of federal agencies, including those in the Intelligence Community. No business could operate effectively with the still-fragmented governance structure that currently guides intelligence activities.

Improving Homeland Security Oversight

The Challenge:

- Creation of the Department of Homeland Security in 2003 brought together 22 existing agencies from multiple departments, which previously answered to more than 80 congressional oversight committees and subcommittees.
- Efforts to streamline Congressional oversight have actually increased the number of committees that claim jurisdiction over the department—to 86 different committees and subcommittees. Since the start of the 110th Congress, Homeland Security officials have testified at 359 hearings and conducted 4,300 briefings for congressional committees -- most for committees other than the House and Senate homeland security committees.
- No successful business could operate effectively and efficiently if it had to answer to 86 different boards of directors—and neither can the Department of Homeland Security.

"Arguably, many of the most significant challenges in effectively managing DHS have resulted from disparate and, at times, contradictory direction from Congress. This has resulted in a plethora of unrealistic mandates and endless tinkering by various congressional committees. Therefore, the first and most productive objective should be to address the lack of effective congressional leadership."

— James Jay Carafano, April 9, 2008, before the House Committee on Homeland Security, Subcommittee on Management, Investigations, and Oversight

The Current Approach:

- In the House of Representatives, the Homeland Security Committee continues to compete with other committees for oversight of key DHS agencies such as the Transportation Security Administration and the Coast Guard.
- In the Senate, the Homeland Security and Government Affairs Committee also shares an oversight role with other committees in addition to managing areas other than homeland security.
- Fragmented congressional oversight will likely hamper the transition to a new administration next year, including confirmation of department leaders and likely changes in budgetary priorities.

A New Approach:

- The House of Representatives should consolidate oversight of all homeland security operations in its Homeland Security Committee.
- Likewise, the Senate should consolidate oversight of homeland security under its Homeland Security and Government Affairs Committee, which should be solely dedicated to homeland security issues.
- To minimize—and hopefully avoid—any disruption to homeland security operations during the transition to a new administration next year, Congress should strive to streamline oversight as quickly as possible.

"Adoption of the 9/11 Commission's recommendation to streamline Congressional oversight of DHS would pay significant productivity dividends. [This is] arguably the most important step Congress can take to improve operational effectiveness at DHS... [and] would allow DHS to focus our time and resources much more effectively on our critical missions, while preserving an appropriate level of Congressional oversight."
— Homeland Security Secretary Michael Chertoff, September 2007

Frequently Asked Questions:

Why does Congressional oversight matter to the average American?
Homeland security deserves the focus and expertise of Congressional oversight. With numerous Congressional committees and subcommittees pursuing separate agendas, the present, fragmented oversight structure provides neither. By developing a single oversight structure, members of Congress can ensure the government is more operationally and financially efficient and – most significantly – strengthen the nation's security.

If oversight is so important, why hasn't Congress already streamlined itself?
Like any large institution, Congress can be slow to reform. Moreover, powerful committee chairmen are reluctant to relinquish their influence over important agencies. But the creation of a single armed services committee in the Senate and House, to oversee the new Department of Defense in 1947, shows that reform is both possible and necessary.

Buying Smarter at the Pentagon

The Challenge:

- Threats to America's national security are emerging and evolving far more rapidly than the Defense Department can harness new capabilities and technologies to meet those threats.
- Despite decades of attempted reforms, it still takes the Pentagon's acquisition system too long – at too great a cost – to develop and deliver new technologies and systems to troops in the field.
- Because the current acquisition system discourages innovation, our troops often receive "yesterday's technology tomorrow" – not the other way around.

"The Government Accountability Office found that 95 major systems have exceeded their original budgets by a total of $295 billion, bringing their total cost to $1.6 trillion, and are delivered almost two years late on average."
— The Washington Post, April 1, 2008

The Current Approach:

- A complex and confusing web of acquisition laws, rules and regulations – many well-intentioned to prevent abuse – has resulted in a system that is slow-moving, risk-averse, and inefficient.
- Recent attempts at reform by Congress have often had the unintended consequences of making the acquisition system even more complicated and less agile.
- Reforms have all focused on the south side of the Potomac River – the Pentagon – and not on the process by which programs are proposed, approved, and overseen in Congress.

A New Approach:

- Rather than continuing to add new layers of statute and regulation, Congress and the Defense Department should embark on a comprehensive effort to dramatically realign the acquisition system and its oversight.
- To foster greater innovation, a balance must be sought between oversight – and the risk aversion it can cause – and acquisition personnel's authority to manage programs that produce real capabilities.
- Congress, the Defense Department, and industry must work together to ensure that programs do not overpromise on results, that cost estimates are realistic, and that funding is stable in order to keep projects on schedule and within budget.

"The [Defense] department expects to invest $900 billion (fiscal year 2008 dollars) over the next five years on development and procurement with more than $335 billion invested specifically in major defense acquisition programs. Every dollar spent inefficiently in acquiring weapons systems is less money for other budget priorities – such as the global war on terror and growing entitlement programs."
— Michael J. Sullivan, Director, Acquisition Management and Sourcing, U.S. Government Accountability Office, April 2008

Frequently Asked Questions:

After so many failed attempts, is it really possible for the Pentagon to change the way it buys things?
Yes. But the key to systemic change includes the Congress. A half-century of accumulated acquisition law must be reviewed and revised if today's dysfunctional system has any hope of being replaced by one that ensures efficiency, accountability, and trust among all parties – Congress, the Executive Branch, the private sector, and American taxpayers.

Don't past abuses argue for more, not less, oversight?
Recent improprieties on a few major acquisitions have some calling for tighter regulation. But such changes, made to prevent recurrence of past abuses, too often create unintended consequences that have detrimental effects even on well-run procurements. In one program, re-regulation caused the delivery schedule to slip 22 months, incurring additional direct costs of $131 million.

Revitalizing Military Bases

The Challenge:

- Despite closing and restructuring hundreds of military bases and facilities since 1988, the military still spends untold billions annually maintaining more bases than it needs.
- In the latest round of base realignment and closure (BRAC 2005), most affected bases were restructured, not closed – often leaving larger bases underused and smaller bases overwhelmed by new missions.
- Local communities are often not equipped to deal with base realignment – the sudden loss of jobs and business after a base closure or downsizing or the sudden increase of missions and manpower when a base is expanded.

"Chanute Air Force Base in Rantoul, Illinois, was closed in 1993. A base redevelopment plan was approved in 1996 with the intent of attracting a United Airlines maintenance facility. The facility, however, never located there. Of 2,125 acres only 16 acres have been transferred to the Village of Rantoul through an Interior Department public benefit conveyance. About one-third of the base was sold to the private sector after closure for residential and commercial-use. ...The Air Force still retains [the other two-thirds] with no intent to reopen the base."

— State of Base Redevelopment Report,
Association of Defense Communities, September 2007

The Current Approach:

- With the latest round of BRAC, the Pentagon eliminated only a fifth of its estimated 20-25 percent excess capacity, draining critical funds away from military readiness and modernization.
- A substantially-downsized base can often be worse than outright closure because it generates less economic activity yet prevents surrounding communities from realizing the full potential of redevelopment.
- In contrast, communities near bases that undergo significant increases in personnel and activities are expected to petition individually the Pentagon, military services, and their representatives in Congress to address local impacts to their schools, roads and other services.

A New Approach:

- To realize the billions of dollars in additional savings from remaining excess bases, the Pentagon should work with Congress for new authorization to close facilities, freeing up funds for American troops.
- To help bases dispose of – and communities develop – vacant properties and facilities, the Defense Department should "pull in the fence posts" by selling or leasing underutilized assets to local communities or commercial, state or federal tenants.
- To help states and communities affected – for better or worse – by realignments, Congress and the administration should create a consistent, nationwide body of law and policy to address the infrastructure and demographic consequences of base closure and realignment.

After years of delay and public debate, the Navy in 2006 auctioned off more than 2,700 acres of the former Marine Corps Air Station at El Toro, California, which was closed in 1999. The El Toro property will become a master planned community with a total of 3,625 homes and 3.0 million square feet of commercial and industrial space, with an additional thousand acres as a federal habitat reserve.
— State of Base Redevelopment Report,
Association of Defense Communities, September 2007

Frequently Asked Questions:

What should I do if the base in our community is closed or restructured?
Remember that a base closure or realignment can be an opportunity. The experience of more than 200 communities affected by earlier closings and realignments shows that redevelopment of older bases can actually create more jobs and greater economic growth than were lost when the base closed or down-sized.

What can our community learn from previous rounds of BRAC?
Local leaders—government and business—should follow the example of other communities:

- Build a regional consensus for an agreed vision of the future;
- Create a local authority to coordinate redevelopment with government and the private sector;
- Evaluate base capabilities to immediately enhance the value of underutilized assets;
- Lobby for state and federal funding for redevelopment.

Recruiting and Retaining the Best People for Government Service

The Challenge:

- With more than 40 percent of the nation's 1.9 million federal employees eligible for retirement over the next decade, the U.S. Government faces the challenge of recruiting more than 100,000 workers every year.
- Competition to match private sector salaries will continue to put intense pressure on the federal budget, where civilian personnel costs already exceed $200 billion per year.
- Despite attempts at reform, the federal government's rigid and outdated pay system has failed to keep pace with the flexibility offered by the private sector.

"Today, less than three percent of the current full-time federal workforce is under the age of 25. To be clear, government's biggest recruiting challenge among young audiences is not attracting sufficient numbers of recent graduates. It is attracting and retaining enough of the most accomplished and skilled young job candidates, and matching them to open positions."
"Making the Difference: A Blueprint for Matching University Students with Federal Opportunities" by The Partnership for Public Service, October 2007

The Current Approach:

- Despite the efforts of some federal departments to replace the government's existing pay system – the General Schedule – with performance-based systems, these efforts are often agency-specific and fail to take into account the best practices from similar efforts elsewhere in government.
- Overly focused on pay and benefits and still assuming "lifetime employment," government personnel systems do not reward performance with greater responsibility or offer the flexibility to enter, leave, and change careers that today's workers expect.
- By often taking six months or more to hire new employees, the federal government struggles to compete with the private sector to recruit qualified college graduates and talented professionals.

A New Approach:

- The federal government should accelerate efforts to replace the outdated pay schedule with a flexible government-wide personnel system that rewards performance with pay scaled to reflect the unique needs of different departments and the special skills needed for different positions.
- To retain highly-skilled employees, government must follow the private sector's lead by increasing opportunities for professional advancement, rewarding employees with greater responsibility, and making it easier for workers to move in and out of public service.
- To improve recruitment, the federal hiring process needs to be dramatically streamlined and include recruitment incentives and the ability to hire employees on a temporary basis to meet urgent needs.

"Implementing more market-based and performance-oriented pay systems is both doable and desirable. Pay increases should no longer be treated as an entitlement but should be based on employees' contributions to the organizations' missions and goals..."
— David M. Walker, Comptroller General of the United States, October 5, 2005

Frequently Asked Questions:

Why does the federal government have a hard time recruiting new employees?
Unlike previous generations of Americans who expected to spend an entire career with a single employer, today's college graduates seek the flexibility to move between different jobs and the opportunity to advance quickly. Those who have considered public service say that government has been slow to reach out to them with opportunities for rapid growth and diverse job opportunities.

Won't the federal government always struggle to compete with the private sector for talented professionals so long as the private sector offers higher salaries?
Government – which serves a public mission – may never be able to offer new hires and senior managers the large salaries of the profit-driven private sector. But many Americans are drawn to government work by the opportunity to serve their country. The federal government will be unable to recruit and retain these civic-minded citizens if it fails to modernize its personnel and pay systems.

Harnessing the Full Strength of America to Promote Global Security

The Challenge:

- Crises from the Balkans to Afghanistan to Iraq show that U.S. national security can require both the "hard power" of military force and – to an even greater degree – the "soft power" of diplomacy, foreign assistance and economic development.
- America's ability to promote political and economic stability around the world through "soft power" has been stymied by the lack of a comprehensive strategy and chronic under-manning and under-funding for our institutions of diplomacy and development.
- As a result, the U.S. military increasingly finds itself performing missions for which it was neither equipped nor trained: building roads and schools, managing public works projects, and overseeing town and city governments.

"Our civilian national security tools are weak, poorly focused and dispersed. Diplomacy and foreign assistance are often underfunded and under used [and] foreign policy institutions are fractured and compartmentalized."
— Center for Strategic and International Studies,
Commission on Smart Power, A Smarter, More Secure America, 2007

The Current Approach:

- The State Department – with an annual budget that is only one percent of the federal budget – lacks the resources and the personnel necessary to fulfill large-scale missions to help stabilize and rebuild strife-torn societies.
- Efforts to bring civilian expertise to conflict zones – such as the successful Provincial Reconstruction Teams in Afghanistan and Iraq – have been ad hoc, difficult to staff and slow to deploy.
- The U.S. government has failed to fully harness the unique experience and expertise of the private sector – including industry and academia – in its missions to revitalize war-torn and struggling business, agricultural, and educational sectors.

A New Approach:

- To relieve the burden on the U.S. military and strengthen America's "soft power," Congress and the next administration should dramatically increase funding for the civilian instruments of national security, including diplomacy, foreign assistance, and economic reconstruction and development.
- To ensure the U.S. is ready for future missions, Congress should support and fully fund a Civilian Response Corps – diplomats, civil affairs officials, aid experts, skilled professionals from across the private sector – ready to deploy rapidly to conflict zones in urgent need of stabilization and reconstruction.
- To magnify the impact of U.S. government professionals, expertise and experience from business, academia, and education should be aggressively enlisted, applied and deployed.

"One of the most important lessons of the wars in Iraq and Afghanistan is that military success is not sufficient to win: economic development, institution-building and the rule of law, promoting internal reconciliation, good governance, providing basic services to the people, training and equipping indigenous military and police forces, strategic communications, and more – these, along with security, are essential ingredients for long-term success."
— Secretary of Defense Robert M. Gates, November 2007

Frequently Asked Questions:

Why have we neglected use of America's "soft power" in our dealings overseas?
As a nation we have failed to develop a vision – shared by the Congress, the President, and the American people – on the potential of using all elements of national power to protect and advance our interests overseas. Until we have this national debate, our efforts will remain piecemeal and ineffective.

Why not simply improve existing capabilities at State and Defense?
Improved capabilities are required, but when activated, the Civilian Response Corps draws manpower from about a half dozen federal agencies and the private sector. With this structure, strategic direction must come from the President, not from a single cabinet official whose authority is limited. Until the Response Corps is activated, management should be at the departmental level.

Business Executives for National Security

For over a quarter century, Business Executives for National Security has been the primary channel through which American business leaders can contribute their special experience and talent to help build a more secure nation.

Founded in 1982 by business executive and entrepreneur Stanley A. Weiss, BENS is guided by the simple notion that America's security is everybody's business. Led by President and CEO General Charles G. Boyd, U.S. Air Force (Ret.), and Board Chairman and real estate executive Joseph E. Robert, Jr., BENS is a highly respected national, nonpartisan organization of senior executives dedicated to enhancing our national security using the successful models of the private sector.

Innovative business-government partnerships that BENS fostered over two decades to help save the Defense Department billions of dollars are now ready to help meet new challenges of the 21st Century. BENS is growing these public-private partnerships into all aspects of homeland security – helping to guard against cyber attack, tracking terrorists' financial assets, securing the nation's ports, and preparing state and local governments to deal with catastrophic events or terrorist attacks.

Recognizing that the nation will never fully realize the efficient, agile military it needs to win a global war on terrorism without an equally efficient and agile support structure, BENS remains a tireless advocate for smarter spending at the Pentagon.

Board of Directors

BENS National
1717 Pennsylvania Avenue, NW, Suite 350
Washington, DC 20006
Website: www.bens.org
E-mail: BENS@bens.org
Tel: (202) 296-2125
Fax: (202) 296-2490

BENS Southeast
BENSSE@bens.org

Kansas City
BENSKC@bens.org

Metro New York
BENSNY@bens.org

Northern California
BENSSV@bens.org

Texas
BENSTX@bens.org

Metro Washington, DC
BENSDC@bens.org

Bay Area Business Force
BayAreaBusinessForce@bens.org

Colorado Emergency Preparedness Partnership
TheCEPP@bens.org

Georgia Business Force
GABusinessForce@bens.org

Homeland Security Advisory Council
(LA and Orange Counties)
HSAC@hsac.bens.org

Safeguard Iowa Partnership
SIP@safeguardiowa.org

MidAmerica Business Force
MidAmericaBF@bens.org

New Jersey Business Force
NJBusinessForce@bens.org

Business Executives for National Security
1717 Pennsylvania Avenue, NW
Suite 350
Washington, DC 20006-4603
www.bens.org